(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2002 (30.05.2002)

PCT

(10) International Publication Number
WO 02/43346 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/EP01/00984

(22) International Filing Date: 31 January 2001 (31.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0028731.8 24 November 2000 (24.11.2000) GB

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RUUTH, Anna-Leena** [FI/FI]; Ankkurinvarsi 12 D 7, FIN-02320 Espoo (FI).

(74) Agents: **JONES, Kendra** et al.; IPR Department, Nokia House, Summit Avenue, Farnborough, Hampshire GU14 0NG (GB).

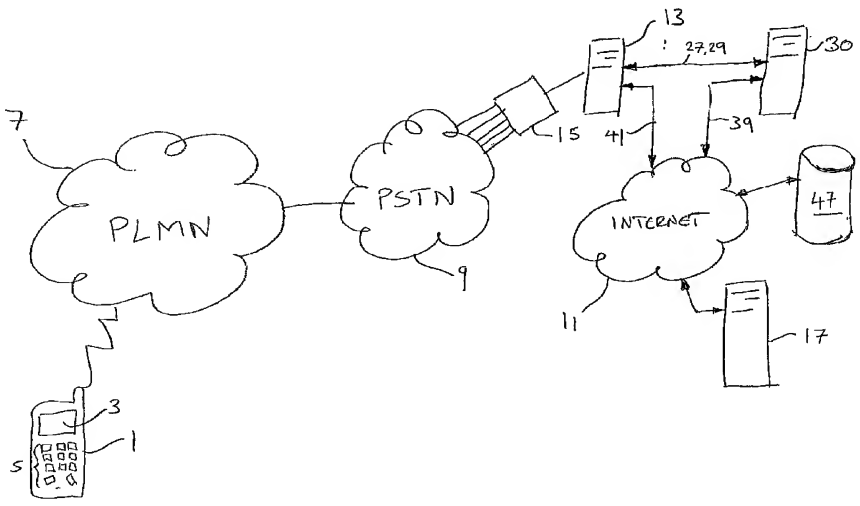
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD, DEVICE AND SYSTEM RELATING TO TRANSACTION SECURITY



(57) Abstract: A device, system and method are described for parsing and propagating end user identity received from a terminal (1) involved in a wireless session to an application in a gateway server (13). The PLMN (7) of which terminal (1) forms part provides access to external networks including a PSTN (9). In addition to conventional telephone operations, the terminal (1) provides its user with access to the internet (11) via the gateway server (13). The gateway server (13) may be operated by a service provider or perhaps a particular organisation such as a bank which for security reasons wishes to keep control of the gateway server (13). Software through which the transactions are carried out is provided by various so-called back-end applications resident on an applications server (17). A trust server (30) is provided which is connectable to the gateway server (13) controlling access to the application server (17).

WO 02/43346 A1

METHOD, DEVICE AND SYSTEM RELATING TO TRANSACTION SECURITY

IMPROVEMENT IN AND RELATING TO TRANSACTION SECURITY

The present invention relates to transaction security, particularly, although not exclusively, in electronic commerce.

The arrival of electronic commerce on a large scale has removed one of the traditional safeguards when carrying out a transaction, namely the physical presence of the parties and/or the means of payment. Whereas, in the past it was at least possible to compare a signature on a credit card or cheque with a specimen or even to present a credit card to a card reader for verification, this is clearly no longer an option when transactions are being carried out remotely as is the case with those transaction taking place over the Internet.

It has been recognised that the different priorities exist for the purchaser and vendor of products/services in Internet based transactions. From the purchaser's perspective, she may be presented with a large number of potential vendors most if not all could be previously unknown to her. When attempting to transact with her selected vendor she will want to be confident that she can trust the vendor. However, unlike a conventional face to face transaction she cannot make any form of assessment of the trustworthiness of the vendor based on the condition of the vendors premises, his staff, other customers and the like. Similarly, the vendor has the difficulty of receiving many requests from people unknown to him all of whom purport to have legitimate means for making payment.

Attempts have been made from each perspective to overcome these problems. Thus, in the case of the purchaser there has been quite universal adoption of a session-based protocol namely the Secure Sockets Layer Protocol. This protocol in its overwhelmingly most common guise permits a

session to be established in which the identity of a server possibly under the control of the vendor is made available in the form of a certificate generated in accordance with the principles of the Public Key Infrastructure (PKI). The purchaser is thus able to assure herself that the server operator has a certificate in which she is prepared to place her trust, the certificate therefore acts as a form of guarantee of the good faith of the server owner.

In the case of the vendor, the approach adopted to resolve the problem has depended largely on the nature of the business relationship with the purchaser. Thus, where a pre-existing relation is in place, perhaps the purchaser is a customer of a bank with which she wishes to carry out a transaction, then one approach has been to provide the purchaser with passwords in the form of shared secrets. Hence, such passwords need to be supplied before a transaction takes place. The provision of passwords before the transaction takes place is clearly not feasible where the transaction is between parties having no pre-existing or continuing relationship. In such a case, the vendor may be forced simply to carry out off-line checks on the validity of credit cards and the like.

According to one aspect of the present invention there is provided a transaction security device for connection to a network including at least one terminal, the device comprising a server operable to validate data provided by a terminal over said connection in order to establish a secure session, the device being operable to respond to a request from said terminal to access an application by obtaining said previously validated data from said server and forwarding said data to said application along with said request.

Advantageously, this merging of the security approach results in increased confidence for both parties to a transaction. The purchaser is no longer reliant merely on the assumption that the vendor is the party behind the session and the vendor has greater confidence in the identity of the purchaser and furthermore in the case of the pre-existing customer relationship, is able

to dispense with the overheads and complexity involved in administering a separate security solution.

According to a further aspect of the invention, there is provided a trust server connectable to a gateway server controlling access to a remote server, the trust server comprising a validator and data storage, wherein the validator is responsive to a first request from said gateway server to deliver status information relating to data received by said gateway server and to store said data in said storage such that said data is retrievable by said gateway server for inclusion in a request to said remote server.

Advantageously, the validation of the data by the server removes the requirement for the extensive data-entry required by application level security. This has the benefit of both reducing the amount of data-entry required from the user and also cutting down on log-in time and the possibility of error. It also removes a perceived barrier to the adoption of electronic commerce, namely that of complexity; if the user believes that too many steps are required to access a service, she will not use it.

According to a still further aspect of the invention, there is provided a transaction security system comprising a server connected to a network including at least one terminal, the server being operable to validate data provided by a terminal over said connection in order to establish a secure session therewith, said server being further operable to respond to a request from said terminal for access to an application by providing said validated data to said application, such that a determination on whether to permit access by said terminal is made by said application in response to said validated data.

Whilst according to a yet further aspect of the invention, there is provided a transaction security method for a server connected to a network, the method comprising acting on a request to establish a secure session over a network

connection including validating data received in said request and following establishment of said session acting on a further request to access an application by providing at least part of said previously validated data to said application for authentication and/or encryption purposes.

In order to aid in understanding the present invention, a particular embodiment thereof will now be described by way of example and with reference to the accompanying drawings, in which:

Figure 1 is a diagrammatic view of a transaction security system according to the present invention;

Figure 2a is a more detailed view of the system of Figure 1 with the intermediate infrastructure omitted for clarity;

Figure 2b is a similar view to Figure 2b with elements of a gateway server omitted for clarity;

Figure 3 is a signal diagram illustrating a method according to the present invention;

Figure 4 is a similar view illustrating further steps in the method of Figure 3;

Figure 5 is a diagrammatic view of the system of Figure 1 in accordance with a further aspect of the invention, and

Figure 6 is a similar view of the system of Figure 1 in accordance with a still further aspect of the invention.

Referring to the Figures and in particular Figure 1, there is shown terminal 1 having a display 3 and a set of keys 5 including alphanumeric keys. Through these keys 5, a user is able, via a user interface, to operate the terminal 1. The terminal 1 forms a mobile element of a Public Land Mobile Network (PLMN) 7 the operation of which will be well known to those skilled in the art. It will noted that the PLMN 7 provides access to external networks including a Public Switched Telephone Network (PSTN) 9.

In addition to conventional telephone operations, the terminal 1 provides its user **U** with access to the Internet 11 via a gateway server 13. The gateway server 13 may be operated by a service provider or perhaps a particular organisation such as a bank which for security reasons wishes to keep control over the gateway server 13. A pool of modems 15 connected to the PSTN 9 provides dial-up access from the terminal side to the gateway server 13. Other access routes may be employed depending on the capability of the terminal 1 and PLMN 7.

As part of its service to customers, an organisation such as a bank **B** allows transactions such as money transfers, share dealing and so on to be carried out electronically using a terminal 1 and an Internet 11 connection. Software through which the transactions are carried out is provided by various so-called back-end applications resident on an applications server 17. Again, for security reasons, the applications server is located in premises of the bank **B**.

In the case of a terminal 1 connected to the PSTN 9, access to a back-end application is provided via the gateway server 13. In this example the gateway server 13 is located on the premises of the bank **B** although there is nothing to prevent locating the gateway server 13 anywhere there is access to the Internet 11. The gateway server 13 facilitates the exchange of information between the terminal 1 and a remote server connected to the Internet and/or intranet, in this case the bank's own back-end applications server 17.

As shown in Figures 2a in further detail, the gateway server 13 comprises a number of functional elements. Firstly, a transport layer block 19 with which the terminal 1 initially negotiates access; secondly, a session data store 21; thirdly, a request handler 23 and fourthly an http-connector 25. Furthermore, these elements have a number of external connections. Thus the transport layer block 19 and request handler 23 are connected 27, 29 to elements of a trust server 30. These elements include a signature validator 31 and a

certificate validator 33. In addition to the external connections 27,29, with the gateway server 13, the trust server 30 has internal connections 35 between the two validators 31,33 and to a configuration store 37 and an external connection 39 between the trust server 30 and the Internet 11. This latter connection 39 permits the trust server 30 to determine the status of information presented to it by the gateway server 13.

Referring again to the gateway server 13, the http-connector 25 is also provided with an external connection 41 to the Internet 11. Through this connection 41 web servers including an application server 17 providing back-end applications may be reached.

As will be further elaborated below, the terminal 1 together with the constituent elements of the gateway server 13 each makes use of the wireless Public Key Infrastructure (wPKI). To enhance further the security provided by the gateway 13, the trust server 30 includes a local cache for both certificates and Certificate Revocation Lists (CRL) 43,45. Regular downloads of CRL are made to the cache from a public directory 47 connected to the Internet 11. The CRLs are signed by appropriate Certification Authority (CA).

Before the terminal 1 can be employed by the user in electronic transactions a number of processes are necessary to establish the security necessary to satisfy both the user and the organisation, in this case the bank **B**, with which she is carrying out her transactions.

Consequently, to enable access to the gateway 13 and the backend applications beyond, the terminal 1 is provided with a tamperproof smart card or token 49 which acts as a carrier for data used to substantiate the identity of the terminal user **U**. During a session, the terminal 1 acts as a conduit for the data stored on the token 49 which is used in securely accessing the relevant back-end application.

The token 49 is manufactured by a card manufacturer which is then delivered to a service provider perhaps the operator of the PLMN, Following delivery, the service provider **SP**, in this case the operator of the PLMN 7, commences personalisation of the token 49 by generating and then storing two unique private/public key pairs on the token 49. Thus there is are provided two private keys and their corresponding public keys, providing respectively, an authentication key and a non-repudiation key. In addition, the service provider root certificate, and URLs pointing to the service provider's **SP** certificates of the public keys are stored on the token 49. The URLs are formed using an identifier of the token 49 as key data. At this stage however, no certificates yet exist. Thus, the URLs on the card are void and therefore unusable.

The user **U** completes personalisation during acquisition of the token 49. Thus, the user **U** personally identifies herself to an authorised employee of the service provider SP using a passport or the like. The employee confirms the completed strong identification of the user with his own digital signature, which is then stored by the service provider. The token 49 is then physically handed over to the user **U** who may now insert it into her terminal 1 for normal mobile telephony purposes. In the meantime, the service provider **SP** associates the identifier of the token 49 with the user's subscription. The service provider **SP** further requests its own Certification Authority (CA) to create certificates for the two public keys on the user's token. The certificates identify the user **U** as the subject of the certificates, and refer to the token identifier. The CA generates the certificates, stores them on the private certificate Directory 47 of the service provider **SP**, and returns an OK response to the service provider **SP**. The service provider **SP** prints from its database the authentication objects or PINs for the two private keys on the token 49, and sends them through the post to the user **U**.

With reference to Figure 3 and Figure 2a, the user **U** is now in a position to be able to register herself as a certified user of the organisation, in this case the bank **B**, with which she wishes to carry out electronic transactions. Thus, the user **U** firstly initiates a call 101 to the access number of a registration service. The terminal 1 physically connects to the dedicated gateway server 13 located in the bank's **B** premises and then attempts to set up a secure session between the terminal 1 and the gateway server 13.

The transport layer block 19 of the gateway server 13 responds 103 by identifying itself with its server certificate and requesting the authentication of the User **U**. Information identifying the bank **B** is derived by the terminal 1 from the gateway server certificate and delivered 104 to the user **U** via the display 3. At the same time, the Terminal 1 requests a response from the user **U** in the form of an authentication PIN1. Using the keypad 5, the user **U** enters 105 her PIN1. Providing the correct PIN1 has been entered the terminal 1 then sends 106 a response to the transport layer block 19 containing the URL of the service provider's certificate of the authentication key, the response having been signed using the authentication key stored on user's token 49.

The transport layer block 19 of the Gateway server 13 forwards the authentication response to request handler 23 which passes it to the certificate validator 33 of the Trust Server 30. As shown in more detail in Figure 5, the certificate validator 33 comprises time critical 51 and non-time critical 53 elements, the first of which, namely the time critical element 51 is activated on receipt of the forwarded authentication response. Hence, the validator 33 identifies the URL containing the service provider's certificate and contacts 108 a corresponding Directory 47 to check the validity of the service provider's certificate for the user **U**. The Directory 47 responds 109 to the Trust Server 30 with information about the certificate and its status such as its validity period. The outcome of the check is reported 110 to the transport

layer block 19 of the trust server. If the status of the certificate is OK, a "session secured" message is sent 111 to the terminal 1 and a secure session is initiated 113, furthermore, the contents of the certificate are stored for the duration of the session in the secure session data store 21. However, before the terminal 1 informs 112 the user **U** via the display 3 that a secure session is now active between the terminal 1 and the gateway server 13, the certificate validator 33 carries out the non-time critical element 53 and accesses the CRL cache 45 in an attempt to determine the revocation status of the certificate. If no certificate is present in the cache 45, a CRL fetch for the information from the CRL directory 47 is initiated. In either case, the revocation status of the certificate is obtained. If the CRL reveals that the certificate has been revoked, a message to this effect is displayed to inform the user **U**. The message may include details of the revoked certificate.

In the event that the certificate has been revoked, the session is terminated. However, should the certificate be in force then the terminal 1 can complete negotiation of the session in accordance with the selected protocol. This may include the generation of shared secrets such as would be understood by those skilled in the art. Whereupon, the terminal 1 is able to send 114 a user authentication request to the registration service of the organisation, in this case the bank **B**.

Referring now in particular to Figure 4, the request is passed by the transport layer block 19 to the request handler 23 which retrieves the contents of the service provider's certificate from the data store 21 and includes them in a header attached to the request. The request, including its header, is then routed by the http-connector 25 via the Internet 11 to the bank registration service which is running on a backend server 17.

The bank registration service recognises the request as being for registration of a user and extracts the certificate data from the request header. The bank

registration service compares the certificate data and in particular the token identity with a customer record directory and seeks to make a match with a previously created record. In the event that no match is found a message to that effect is delivered to the terminal and the session is closed. However, if a match is made the bank registration service responds by sending 115 an acknowledgement text together with a request that the user **U** enters her non-repudiation PIN2 at the Terminal 1 to confirm her identity (see Figure 2b).

The terminal 1 displays 116 the text and the user **U** duly enters 117 her non-repudiation PIN2 using the keypad 5 of the terminal 1. Assuming the PIN2 is correctly entered, the terminal 1 uses the private non-repudiation key on the token 49 to sign the response in the manner known to those skilled in the art of asymmetric cryptography. The response is sent 118 via the gateway server 13 (not shown) to the backend server 17 running the bank registration service. The bank registration service receives the response and forwards 119 it to the Trust Server 30 for the authentication of the signature by the signature validator 31. The signature validator checks the signature in the received message using the public certificate of the non-repudiation key in the manner well known to those skilled in the art of asymmetric cryptography. Thus, the trust server obtains the certificate by requesting 120 it from the Directory 47containing the non-repudiation public key. The Directory 47 provides 121 the trust server 30 with the certificate details and the trust server 30 returns 122 the results of its analysis of the signature to the bank registration service.

If the status of the certificate was OK and the signature itself was OK, the bank registration service requests 123 that the Trust Server 30 checks whether there already exist Bank certificates for the user's token 49. The Trust Server 30 interrogates 124 the Bank's certificate Directory 47 to determine whether there are certificates associated with the token 49. The token identifier contained in the header with the original registration request from the terminal 1 is thus used as the search term in this query. The

directory 47 returns 125 its data to the trust server 30. If, as a result of this check by the trust server 30, the trust server 30 informs 126 the bank registration service that there were already certificates associated with the user's token 49 in the Bank's certificate Directory 47, the terminal is informed 127 and a corresponding message is displayed 128 by the terminal 1 and the user **U** is informed that the registration has already been done and the registration session is closed. Otherwise, the bank registration service requests an update 128 of the Customer record directory with the information that a token 49 holding the certificates of the Bank is a valid authentication method for the user **U**.

Subsequently, the bank registration service causes an "authentication successful" message to be delivered to the terminal 1. The user is then able to read 131 a message generated 130 on the display 5 informing the user that registration was successful and that it will be completed after the Bank's certificates have been sent to the user's terminal 1.

Delivery of the certificates may take place by any suitable method including over the air using a SMS route, by a push session either originated by the bank registration service or indeed whilst the registration session is still active.

The user **U** is now in a position to be able to access the transactional facilities made available to her by the bank **B**, but using the bank's certificates to establish a secure session over the gateway server 13 to the backend transaction application of the bank **B**. In some cases such as simple balance enquires and the like it maybe sufficient only for the transactional application to be satisfied that the session has been established using a valid bank certificate in accordance with the process described above in relation to the service provider certificate including a check to determine whether the bank certificate has not been revoked. However, where a more sensitive transaction is being carried out, such as the transfer of money between

accounts or making a trade, then the transaction application may, as a further security step, request that a transaction acknowledgement be signed by the User **U** using her non-repudiation PIN2 to cause the terminal 1 to sign the acknowledgement using the non-repudiation key which may then be checked by the trust server 1 as previously described above including checking the CRL to determine the revocation status of the certificate relating to the non-repudiation key.

It may well be the case that a gateway server 13 is required to provide access to a plurality of applications operated by different organisations (Figure 6). The owner of the gateway server 13 could be an organisation such as a bank which could provide the facility to other organisations reluctant or enable to invest in establishing their own gateway. As such, the server 13 is required to provide access not only to applications corresponding to those already described but also to so-called legacy applications. Such a legacy application may be incapable of extracting certificate information from the header of a request passed to it by the http-connector module 25.

Hence, the gateway server 13 further includes an access control module 55 which interprets the received request from a terminal 1 and queries the session data store 21 which may also hold details of access rights and the like for the applications accessible from the gateway 13. Preferably however, the access rights are stored permanently outside of the session data store 21. This information may be pre-stored, or could be created dynamically following a failure to communicate certificate information to an application in the manner previously described.

Thus, following the authentication of a user as described previously, the ensuing request from the terminal 1 is interpreted by the access control module 55 which establishes firstly whether authorisation of the user is required as might be the case for the abovementioned legacy applications. If

not, the access control module then passes to the next stage of identifying the access rights including the URLs necessary to access the application on the back-end server 17. As previously described, the request handler then places the certificate information together with any information intended to be included from the data store in a header to the request. The subsequent processing of the request then follows the steps previously described including the CRL check and the optional non-repudiation step.

Alternatively, if the application is identified by the access control 55 as a legacy application, then the access module 55 optionally initiates an authorisation step. Whether such a step is required is determined by the access control module 55 which has access to the data store 21 and the particular records for that application. For example, the records may include, in the form of a profile, how the owner of an application wishes particular requests to be handled. In order to authorise the user; a request is sent to the terminal 1 which displays a message asking the user to enter her non-repudiation PIN2. Once the PIN2 has been correctly entered, the terminal 1 signs the response using the non-repudiation private key and sends the response to the gateway server 13 where it is intercepted by the access control module 55. The access control module 55 asks the request handler 23 to contact the trust server 30 whose signature validator 31 validates the signature against the relevant certificate. Assuming the signature is validated then the access control module 55 allows the original request from the terminal to be passed to the http-connector 25 and thus to the back-end server 17' on which the legacy application is resident, but not before the certificate has been checked against the CRL cache as described above.

It will be appreciated by those skilled in the art that no reference has been made to a particular protocol for use in establishing a secure session between a terminal and a gateway server. One example of such a protocol is the Wireless Transport Layer Security Specification (WTLS) dated 18 February

2000, which specification forms part of the Wireless Application Protocol published by the Wireless Application Protocol Forum. Similarly an example of one particular embodiment of a token is that set out in another specification published by the Wireless Application Protocol Forum, namely the Wireless application protocol Identity Module (WIM) dated 5 November 1999. The cryptographic tools necessary to provide the functionality set out in the above description are well known to those skilled in the art of asymmetric cryptography, nevertheless, the particular tools required to provide such functionality in the case of the WAP protocol may be further studied in the specification published by the Wireless Application Protocol Forum, namely the WMLScript Crypto Library dated 5 November 1999. Furthermore, the skilled addressee will recognise that the initial registration process outlined in the embodiment is but one of many available. One such alternative process might be to utilise self-signed certificates rather than have them issued by a service provider.

CLAIMS

1. A trust server connectable to a gateway server controlling access to a remote server, the trust server comprising a validator and data storage, wherein the validator is responsive to a first request from said gateway server to deliver status information relating to data received by said gateway server and to store said data in said storage such that said data is retrievable by said gateway server for inclusion in a request to said remote server.

2. A trust server as claimed in Claim 1, wherein the remote server provides access to one or more applications.

3. A trust server as claimed in Claim 1 or Claim 2, wherein the data is received from a terminal.

4. A trust server as claimed in Claim 3, wherein the terminal is a mobile station.

5. A trust server as claimed in any preceding Claim, wherein the data is received from an application.

6. A trust server as claimed in any preceding Claim, wherein the data comprises a public key certificate.

7. A trust server as claimed in Claim 6 as appendant to Claim 3, wherein the private key corresponding to said public key certificate is stored on said terminal.

8. A trust server as claimed in Claim 7, wherein the private key is stored within a token.

9. A transaction security device for connection to a network including at least one terminal, the device comprising a server operable to validate data provided by a terminal over said connection in order to establish a secure session, the device being operable to respond to a request from said terminal to access an application by obtaining said previously validated data from said server and forwarding said data to said application along with said request.

10. A device as claimed in Claim 9, wherein the data comprises a public key certificate.

11. A device as claimed in Claim 10, wherein the private key corresponding to said public key certificate is stored on said terminal.

12. A device as claimed in Claim 11, wherein the private key is stored within a token.

13. A device as claimed in any one of Claims 9 to 12, wherein the terminal is a mobile station

14. A transaction security system comprising a server connected to a network including at least one terminal, the server being operable to validate data provided by a terminal over said connection in order to establish a secure session therewith, said server being further operable to respond to a request from said terminal for access to an application by providing said validated data to said application, such that a determination on whether to permit access by said terminal is made by said application in response to said validated data.

15. A system as claimed in Claim 14, wherein the data comprises a public key certificate.

16. A system as claimed in Claim 15, wherein the private key corresponding to said public key certificate is stored on said terminal.

17. A system as claimed in Claim 16, wherein the private key is stored within a token.

18. A system as claimed in any one of Claims 14 to 17, wherein the terminal is a mobile station.

19. A transaction security method for a server connected to a network, the method comprising acting on a request to establish a secure session over a network connection including validating data received in said request and following establishment of said session acting on a further request to access an application by providing at least part of said previously validated data to said application for authentication and/or encryption purposes.

20. A method as claimed in Claim 19, including generating said secure session request in a terminal connected to said network.

21. A method as claimed in Claim 19 or Claim 20, including generating said application access request in a terminal connected to said network.

22. A method as claimed in any one of Claims 19 to 21, wherein the data comprises a public key certificate.

23. A method as claimed in Claim 22 as appendant to Claim 20, wherein the private key corresponding to said public key certificate is stored on said terminal.

24. A method as claimed in Claim 23, wherein the private key is stored within a token.

25. A method as claimed in Claim 23 and any Claim dependant therefrom, wherein the terminal is a mobile station.

26. A computer program comprising executable code for execution when loaded on a computer, wherein the computer is operable in accordance with said code to carry out the method according to any one of Claims 19 to 25.

27. A program as claimed in Claim 26, stored on a computer readable medium.

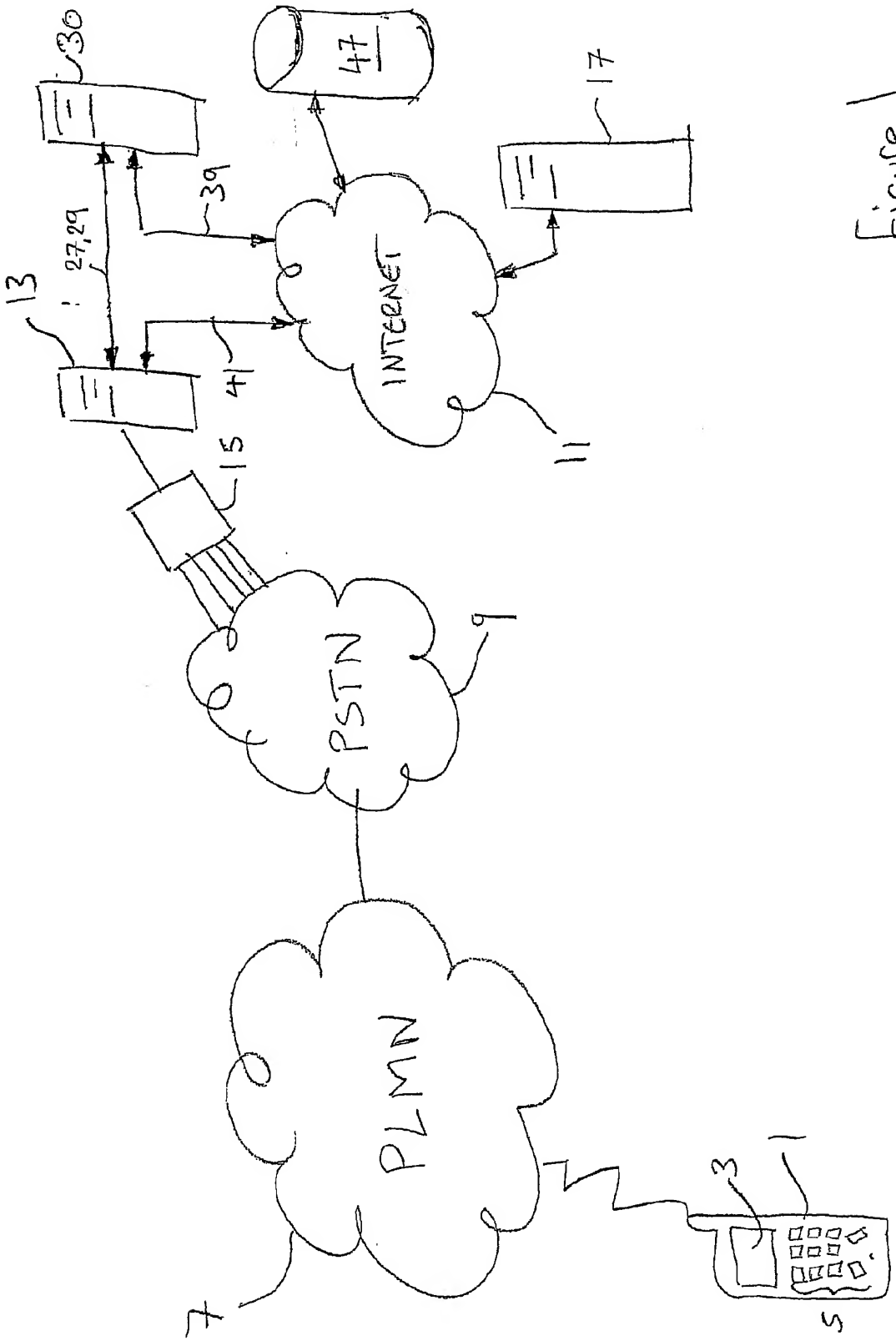


Figure 1

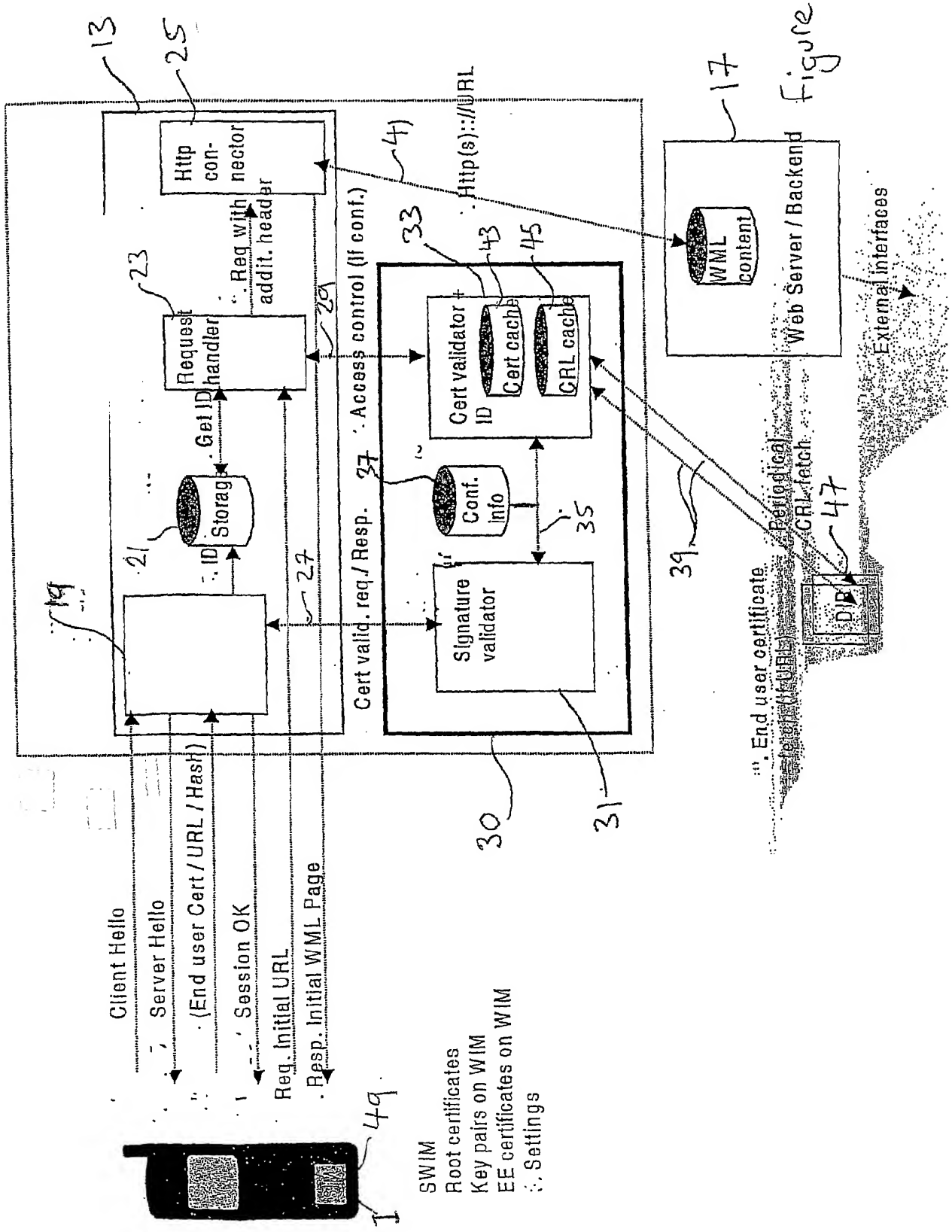

Client Hello
Server Hello
(End user Cert / URL / Hash)
Session OK
Req. Initial URL
Resp. Initial WML Page
SWIM
Root certificates
Key pairs on WIM
EE certificates on WIM
Settings
Storage
Get ID
Request handler
Req with addit. header
Http con-nector
Cert valid. req./ Resp.
Access control (If conf.)
Conf. info
Signature validator
Cert validator + ID
Cert cache
CRL cache
Http(s)://URL
WML content
Web Server / Backend
External interfaces
End user certificate
Periodical CRL fetch
DP
13
17
19
21
22
23
25
26
27
30
31
33
35
37
39
41
43
45
47
49

Figure 2a

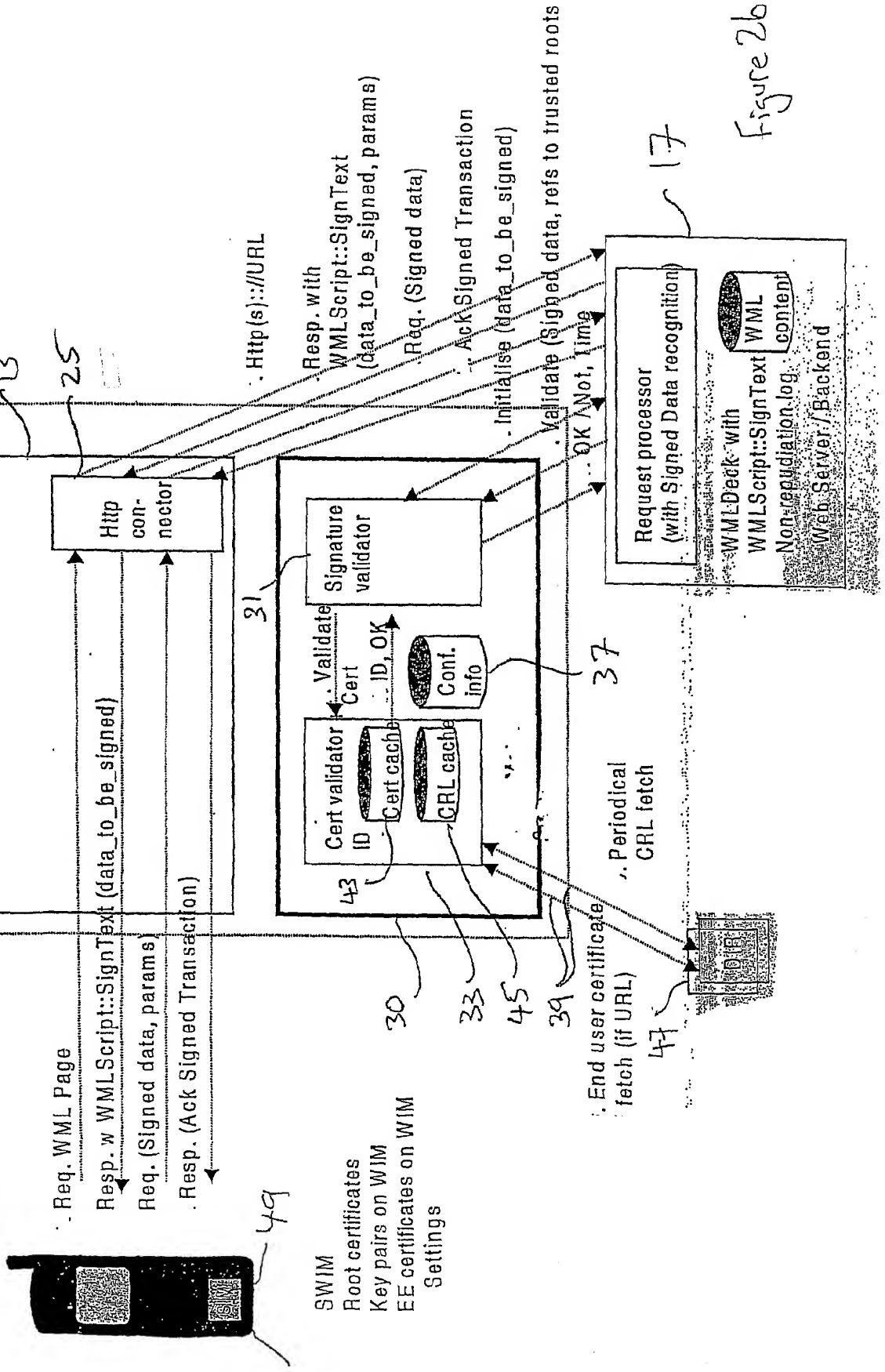

. Req. WML Page
Resp. w WMLScript::SignText (data_to_be_signed)
Req. (Signed data, params)
. Resp. (Ack Signed Transaction)
SWIM
Root certificates
Key pairs on WIM
EE certificates on WIM
Settings
. End user certificate fetch (if URL)
. Periodical CRL fetch
. Http(s)::://URL
Resp. with WMLScript::SignText (data_to_be_signed, params)
Req. (Signed data)
. Ack Signed Transaction
. Initialise (data_to_be_signed)
. Validate (Signed data, refs to trusted roots
. OK / Not, time
Http con-nector
Signature validator
. Validate Cert
. ID, OK
Cert validator ID
Cert cache
CRL cache
Cont. info
Request processor (with Signed Data recognition)
WMLDeck with WMLScript::SignText
WML content
Non-repudiation log
Web Server / Backend
13
25
31
43
30
33
45
39
37
47
49
17

Figure 2b

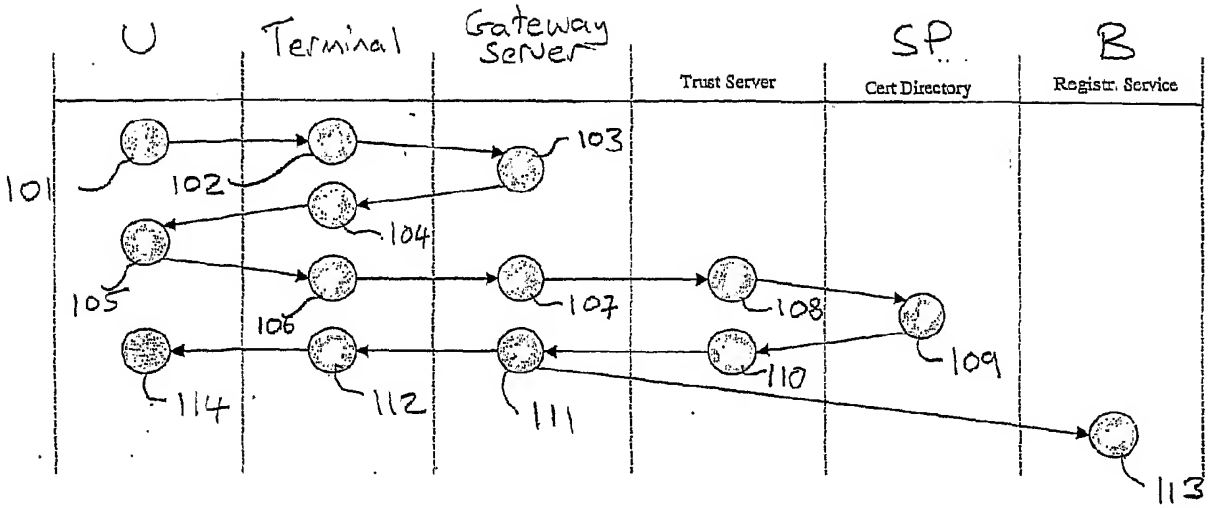


Figure 3

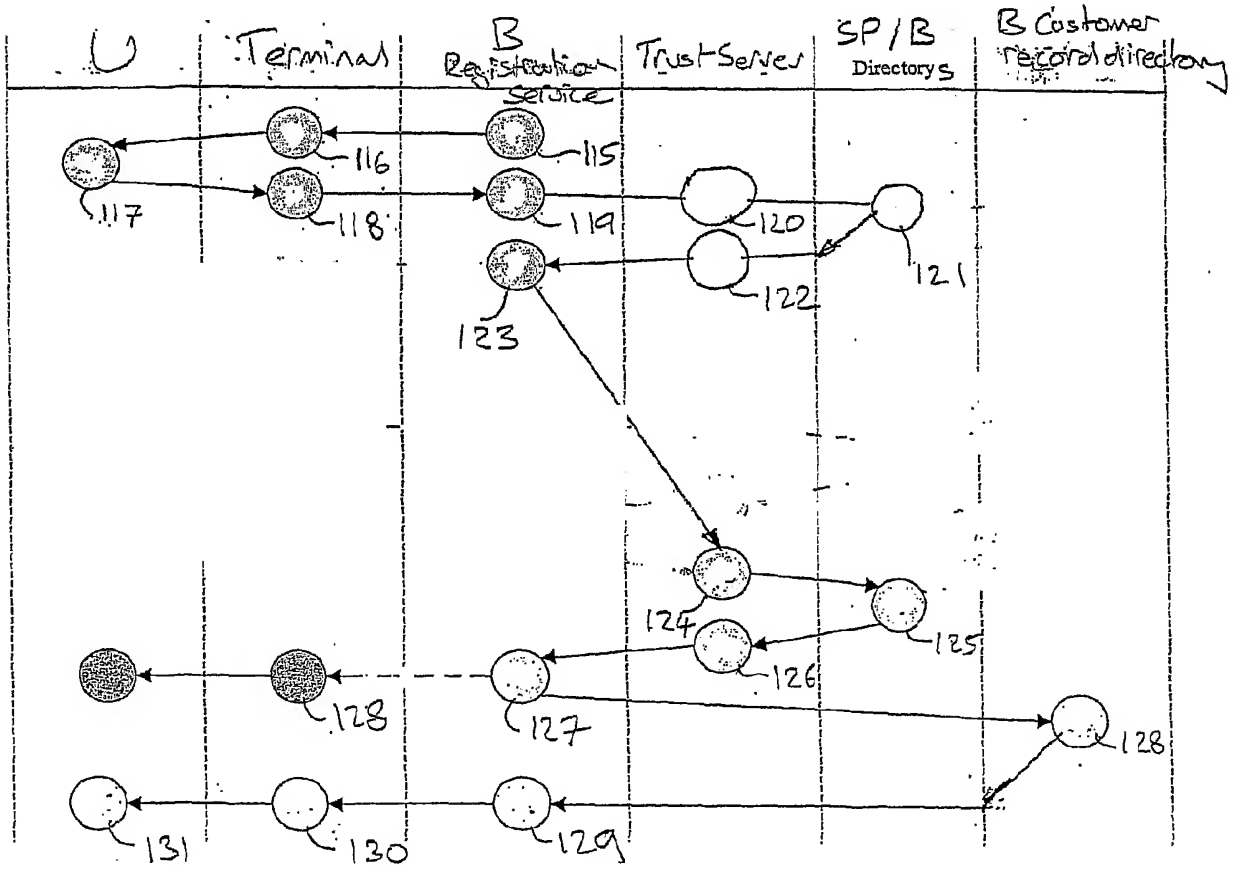


Figure 4

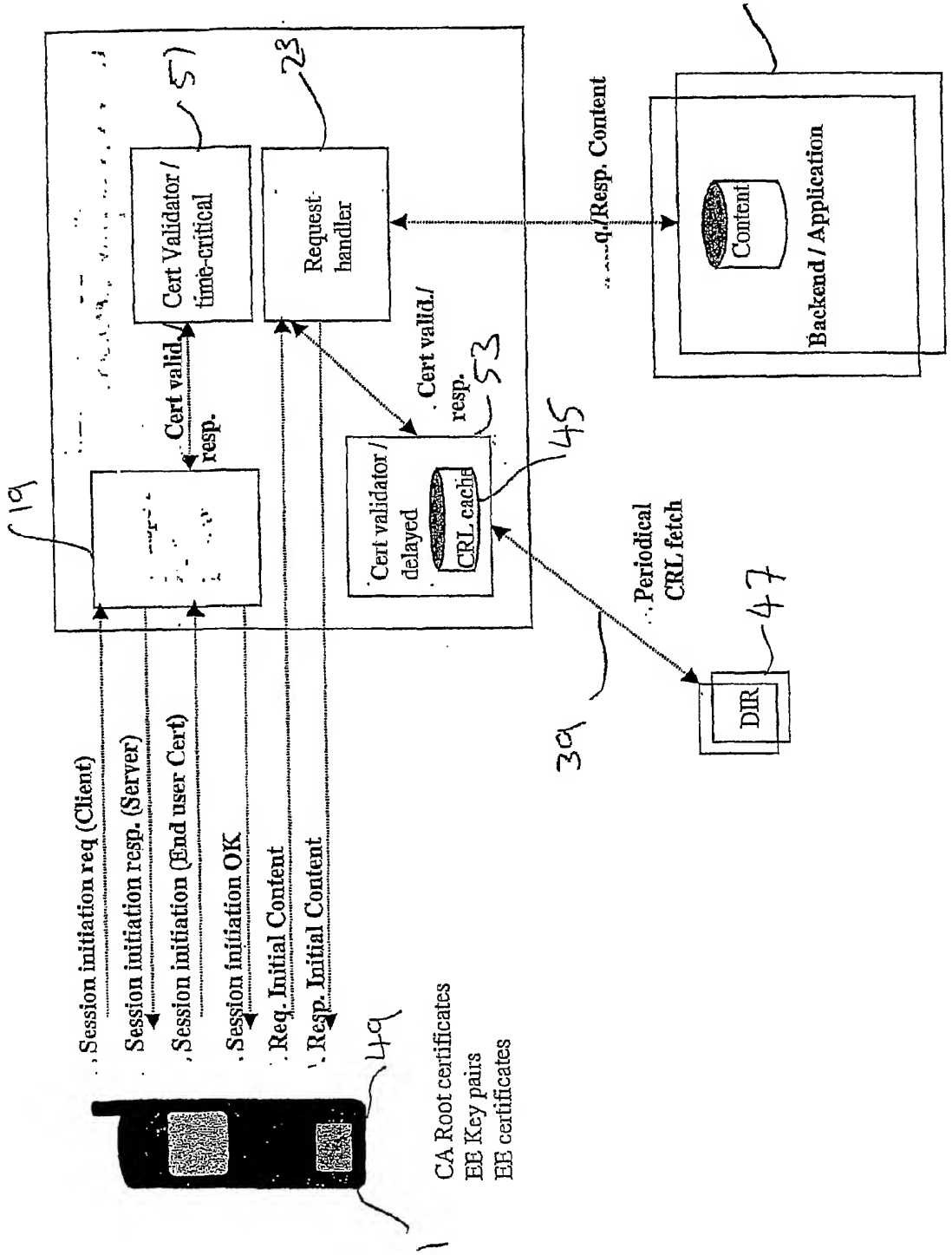

Session initiation req (Client)
Session initiation resp. (Server)
Session initiation (End user Cert)
Session initiation OK
Req. Initial Content
Resp. Initial Content
CA Root certificates
EE Key pairs
EE certificates
49
1
19
Cert valid./ resp.
Cert Validator / time-critical
51
23
Request handler
Cert valid./ resp.
53
Cert validator / delayed
CRL cache
45
Periodical CRL fetch
39
DIR
47
q./Resp. Content
Content
Backend / Application
17

Figure 5

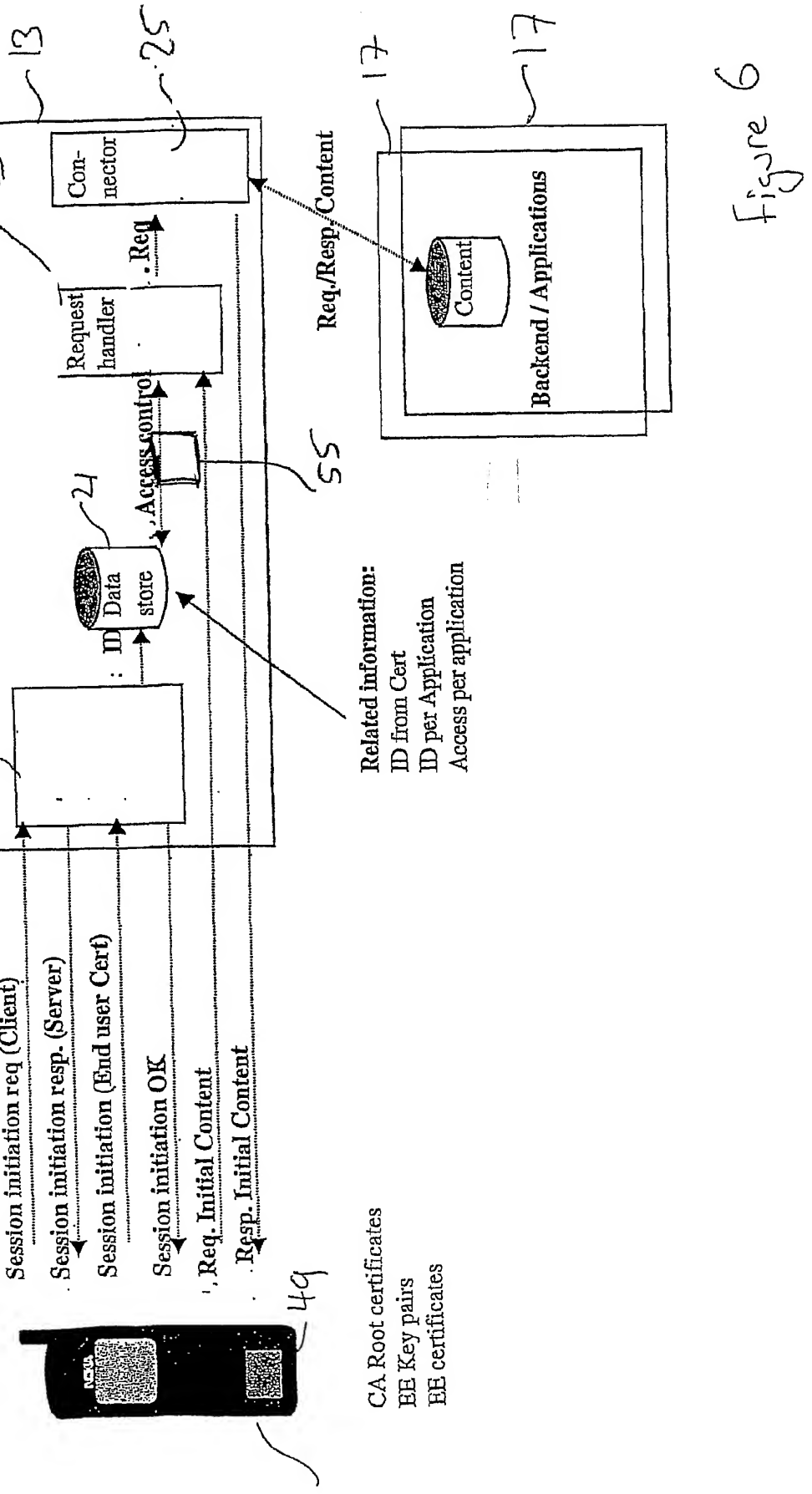

13
25
23
Con-
nector
Request
handler
Req
Access control
24
ID
Data
store
19
55
17
17
Req./Resp. Content
Content
Backend / Applications
Related information:
ID from Cert
ID per Application
Access per application
Session initiation req (Client)
Session initiation resp. (Server)
Session initiation (End user Cert)
Session initiation OK
Req. Initial Content
Resp. Initial Content
49
CA Root certificates
EE Key pairs
EE certificates

Figure 6

INTERNATIONAL SEARCH REPORT

Application No
PCT/EP 01/00984

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 36522 A (GTE LABORATORIES INC) 20 August 1998 (1998-08-20) page 8, line 7 -page 9, line 11 page 13, line 1 -page 16, line 9 figures 1,3,4,6	1-3,5
Y		4,6-8
Y	WO 99 16029 A (NOKIA TELECOMMUNICATIONS OY ;HIPPELAEINEN LASSI (FI)) 1 April 1999 (1999-04-01) figure 2 page 8, line 26 -page 9, line 36	4,6-8

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 October 2001	26. 10. 01

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Körbler, G

INTERNATIONAL SEARCH REPORT

Int Application No
PCT/EP 01/00984

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 105 131 A (CARROLL ROBERT B) 15 August 2000 (2000-08-15) column 1, line 53 -column 2, line 25 column 2, line 49 -column 3, line 49 column 6, line 39 -column 6, line 62 column 7, line 21 -column 9, line 54	9-11, 14-16, 19-23, 26,27
Y	figures 1,3A,3B,3C,5,6	12,13, 17,18, 24,25
Y	WO 00 02358 A (NOKIA MOBILE PHONES LTD ;IMMONEN OLLI (FI)) 13 January 2000 (2000-01-13) page 7, line 5 -page 9, line 30 figure 2	13,18,25
Y	US 5 903 721 A (SIXTUS TIMOTHY) 11 May 1999 (1999-05-11) column 2, line 66 -column 3, line 3	12,17,24
A	PAYS P ET AL: "An intermediation and payment system technology" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 28, no. 11, 1 May 1996 (1996-05-01), pages 1197-1206, XP004018220 ISSN: 0169-7552 sections 2.4-3.3 page 1198, right-hand column -page 1204, left-hand column	9-27

INTERNATIONAL SEARCH REPORT

ional application No.
PCT/EP 01/00984

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-8

   trust server connectable to a gateway server controlling access to remote server.

2. Claims: 9-27

   transaction security device , system, method and computer program comprising a connection to a network including at least one terminal, the device comprising a server in order to establish a secure session.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int[illegible]plication No
PCT/EP 01/00984

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9836522	A	20-08-1998	US	5923756 A	13-07-1999
			EP	0960500 A1	01-12-1999
			JP	2001511982 T	14-08-2001
			WO	9836522 A1	20-08-1998
			US	6198824 B1	06-03-2001
			US	2001020274 A1	06-09-2001
WO 9916029	A	01-04-1999	FI	973788 A	26-03-1999
			AU	9351498 A	12-04-1999
			CN	1271449 T	25-10-2000
			EP	1018098 A1	12-07-2000
			WO	9916029 A1	01-04-1999
US 6105131	A	15-08-2000	NONE		
WO 0002358	A	13-01-2000	AU	4781899 A	24-01-2000
			CN	1316152 T	03-10-2001
			WO	0002358 A1	13-01-2000
			EP	1095492 A1	02-05-2001
US 5903721	A	11-05-1999	AU	6549498 A	29-09-1998
			DE	1008022 T1	25-01-2001
			EP	1008022 A2	14-06-2000
			ES	2150892 T1	16-12-2000
			NO	994428 A	09-11-1999
			WO	9840809 A2	17-09-1998